Compliance Component

DEFINITION	
Name	Disposal Phase
Description	The disposal phase of the agency information system life cycle includes the disposition of information, media and software.
Rationale	The disposal phase is essential to prevent the inadvertent release of data, information, or software.
Benefits	• Protect sensitive information from disclosure. • Adhere to copyright, statutory, and regulatory requirements.
ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Management Controls
List the Technology Area Name	System Life Cycle Security
List Product Component Name	CyberCide, DataGone, DBAN, DiskWipe, East-Tec, Eraser, FDisk, GDisk, KillDisk, WipeDrive
COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	
COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	• Official electronic records shall be properly archived or disposed using approved methods. • Obsolete, surplus or decommissioned media shall be overwritten, degaussed, or destroyed. o **If the information contained on a disk or hard drive is of such a sensitive nature that inadvertent release of the information would be catastrophic, the media must be physically destroyed.** • A record shall be kept of who, when, and how sanitization or disposal actions were implemented on all computers and shall be maintained within the organization for an appropriate length of time. o **Sanitizing (also called purging or wiping) means removing all traces of information from a disk or hard drive in a manner that gives reasonable assurance that the information is unrecoverable.** • If the sanitization status of a computer or storage media is unknown, it shall be considered not to have been overwritten

or degaussed.

- The owner shall be responsible for backing up any data to be retained before allowing the media to be disposed.

Overwriting Hard Drives

- Overwriting software shall provide the capability to:
  - Purge all data or information, including the O/S, from the physical or logical drives.
  - Run independent of the loaded O/S on the hard drive and the type of hard drive being sanitized, e.g., ATA/IDE or SCSI type hard drives.
  - Overwrite all sectors, blocks, tracks, and slack or unused disk space on the entire hard disk medium.
  - **Raid controlled hard drives must be individually wiped.**
  - Verify that all data has been removed from the entire hard drive and the ability to view the overwrite pattern.
  - Provide the user with validation that the procedure was completed properly.
- Overwriting software that merely reformats or repartitions a hard drive is not acceptable.
- The overwriting process shall be performed at least three times before verifying the media is sanitized.
- If damaged hard drives inhibit the overwriting process, the storage media shall be physically destroyed or returned to the vendor, if appropriate non-disclosure agreements have been signed.

Destroying Damaged Hard Drives

- Damaged hard drives under maintenance agreements may be returned to the vendor if appropriate non-disclosure agreements have been signed.
- Hard drives may be physically destroyed by one of the following methods:
  - Disfigure, bend, mangle, or otherwise mutilate the hard drive so that it cannot be re-used by a functioning computer.
  - Destroy the hard drive at an approved metal destruction facility, i.e., smelting, disintegration, or pulverization.
  - Apply an abrasive (emery wheel or disk sander) to the entire recording surface of a magnetic disk or drum.

Degaussing Removable Media

- Degaussers shall have a nominal rating of at least 1700 Oersted and shall be operated at their full magnetic field strength.
- Shielding materials shall be removed from the hard drive and

	magnetic platters shall be removed from the hard drive housing before degaussing. • Individuals performing the degaussing function shall be properly trained.		
Document Source Reference #	NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems; NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems; NIST SP 800-53 (draft) Recommended Security Controls for Federal Information Systems (www.csrc.nist.gov/publications/nistpubs); DOD 5220.22-M, Department of Defense Clearing and Sanitization Matrix		
Standard Organization			
Name		*Website*	
Contact Information			
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
KEYWORDS			
List all Keywords	Wipe, erase, clean, expunge, obliterate, purge, salvage, surplus, confidential, sanitize		
COMPONENT CLASSIFICATION			
Provide the Classification	☐ *Emerging* ☒ *Current*	☐ *Twilight*	☐ *Sunset*
Rationale for Component Classification			
Document the Rationale for Component Classification			
Conditional Use Restrictions			
Document the Conditional Use Restrictions			
Migration Strategy			
Document the Migration Strategy			
Impact Position Statement			
Document the Position Statement on Impact			
CURRENT STATUS			
Provide the Current Status)	☐ *In Development* ☐ *Under Review*	☒ *Approved*	☐ *Rejected*
AUDIT TRAIL			
Creation Date	07/22/2004	*Date Accepted / Rejected*	07/30/2004

Reason for Rejection			
Last Date Reviewed	12/23/2004	*Last Date Updated*	12/23/2004
Reason for Update	Added bullet about destroying drive if highly sensitive info.		